APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/572,900	03/21/2006	Alfred Boucek	2003P14866WOUS	2994

22116   7590   07/10/2008
SIEMENS CORPORATION
INTELLECTUAL PROPERTY DEPARTMENT
170 WOOD AVENUE SOUTH
ISELIN, NJ 08830

EXAMINER
TABOR, AMARE F

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
07/10/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

	Application No.	Applicant(s)
Office Action Summary	10/572,900	BOUCEK ET AL.
	Examiner	Art Unit	
	AMARE TABOR	2139	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>02 April 2008</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>12,14,16 and 24-26</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>12,14,16 and 24-26</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>31 March 2006</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   This correspondence s in response to **Amendments** and **REMARKS** filed on April 02, 2008.

2.   Claims 13, 15 and 17-23 are cancelled [Claims 1-11 were previously cancelled]. Claims 12, 16

and 24 are amended. Claims 14 and 26 are previously presented.

3.   **Claims 12, 14, 16 and 24-26** are pending.

Response to Arguments

4.   Applicant's arguments filed on 04/02/2008 have been fully considered but they <u>are not</u>

persuasive.

Applicants argued:

"*…it is felt that Yoshimoto and Senapati, singly and in combination, fail to teach or to suggest*

authenticating a session via the subscriber's connection by using the combination of the

connection data and the subscriber data contained in the discovery messages…"

Examiner respectfully disagrees.

Yoshimoto discloses the claim of "*authenticating a session via the subscriber's connection by*

using the combination of the connection data and the subscriber data" as, [abstract, "*…a server receives*

a service request from a client, <u>identifiers of a terminal and of a user are acquired</u> from the service

request and <u>authority with respect to the service request is uniquely decided from the terminal and user</u>

<u>identifiers acquired. It is then…</u>"] In other words, Yoshimoto discloses a service request [**a session**] that

is uniquely decided [**authenticated**] by using terminal identifiers [**connection data**] and user identifiers

[**subscriber data**]. This authentication of a session using the terminal and user identifiers jointly is clearly

seen in FIGS.2-5. Specifically, FIGS.2 and 3 disclose authenticating a SERVICE [or CONNECTION]

REQUEST after ACQUIRING TERMINAL and USER IDENTIFIERS from the session.

Similarly, Senapati discloses authenticating a session using two identifiers jointly. See for example, abstract, "...*A PPPoE session is established, and <u>an authentication request is transmitted, containing the **identifier** and a generic **password**</u>, from the modem to a single configuration domain name over the PPPoE network. Authorization is then received from the configuration...*"

Specification

5.   The amendment filed on 04/02/2008 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: independent **claims 12 and 25** recite, "*...at least <u>a discovery stage</u> to establish a session based on data, supplied in one or more discovery messages...inserting...data as respective tags in said one or more discovery messages...*" However, '**discovery stage**' is <u>not</u> disclosed in the specification.

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Objections

6.   <u>Claim 24</u> is objected to under 37 CFR 1.75(c) as being in improper form because it <u>does not</u> refer back to another claim [but refers to a succeeding claim, 25]. See MPEP § 608.01(n). Accordingly, the claim has not been further treated on the merits.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 12, 14, 16 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over
"**Yoshimoto**" (US 6,237,023 B1) in view of Senapati et al. (US 2003/0041151 A1, referred as
"**Senapati**")

    As per Claim 12, Yoshimoto teaches,

    A method for performing data transmission via a subscriber's connection located in an Ethernet
communication network [see network cable **101** in FIG.1; and for example, col.3, lines 42-47, "*As shown
in FIG. 1, a group of terminals, described later, are connected to a **network cable 101** to construct a
computer network. The computer network described here includes **an Ethernet**, a LAN using an FDDI, a
WAN constructed by interconnecting networks by a public telephone line or leased line, etc*"] the method
comprising: defining a connection data [see abstract], wherein the connection data includes a port
identification that uniquely identifies a subscriber's connecting line corresponding to the subscriber's
connection [see **ACQUIRE TERMINAL IDENTIFIER FROM SERVICE REQUEST S201** in FIG.2,
ACQUIRE TERMINAL IDENTIFIER FROM CONNECTION REQUEST S301 in FIG.3 and **IDENTIFIER
ACQUSITION MODULE** in FIGS.6 and 7];

    transmitting the connection data and the subscriber data via the subscriber's connection in
accordance with a predefined protocol for the Ethernet communication network comprising at least a
discovery stage to establish a session based on data, supplied in one or more discovery messages [see
FIGS.1-5 – *where Yoshimoto discloses transmitting client's service requests to server over network
connection cable 101*]; and

    authenticating [see **AUTHENTICATION SERVER** in FIG.1] a session [**service/connection
request**] via the subscriber's connection by using the combination of the connection data [**terminal
identifier**] and the subscriber data [**user identifier**] contained in said one or more discovery messages
[see **SERVICE/CONNECTION REQUEST** in FIGS.2-5], wherein the session is established upon a joint
verification [see **DECIDE CORRESPONDING AUTHORITY OF SERVER TERMINAL** in FIGS.2-5] of the
connection data and the subscriber data which in combination identify the subscriber's connection, said
joint verification of the connection data and the subscriber data [see FIGS.2-5] enhancing a likelihood of

accurately authenticating the session through the subscriber's connection [see for example, col.1, lines 59

to col.2, line6, "…*an object of the present invention is to provide an access control system and method in*

which, when shared resources in a distributed system are accessed, the shared resources can be

protected safely and flexibly… the foregoing object is attained by providing …. acquisition means for

acquiring an identifier of a terminal-which requests a service and an identifier of a user, decision means

for uniquely deciding authority over the service request based upon the terminal identifier and user

identifier that have been acquired, and judging means for judging, using the authority that has been

decided, whether or not to accept the service request"].

        Yoshimoto discloses defining a subscriber data including user identifier [see **ACQUIRE USER**

IDENTIFIER FROM SERVICE REQUEST S202-S401 in FIGS.2 & 4, **ACQUIRE USER IDENTIFIER**

FROM CONNECTION REQUEST S302-S501 in FIGS.3 & 5 and **IDENTIFIER ACQUSITION MODULE** in

FIGS.6 and 7], wherein the connection data and the subscriber data in combination uniquely identify the

subscriber's connection [see abstract – *where Yoshimoto discloses terminal and user identifiers uniquely*

identifying service requests]; but fails to disclose a user name and a password, and inserting the

connection data and the subscriber data as respective tags in said one or more discovery messages to

the communication network via the subscriber's connection.

        However, in the same filed of endeavor, Senapati discloses a user name and a password [see

Generic Password 234, User Identifier 238, Usernames 240, …in FIG.2]; and for example, abstract,

par.0009, 0016, 0020, 0050, 0051, 0072, …], and inserting the connection data and the subscriber data

as respective tags in said one or more discovery messages to the communication network via the

subscriber's connection [see **Modem 104** in FIGS.1 and 2; and for example, par.0047 and 0063-0071 of

Senapati].

        Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of

Applicants' invention, to combine the teachings of Yoshimoto and Senapati because both are in the fields

of authenticating data transmission. Incorporating Senapati's teaching modifies the system of Yoshimoto,

so that security of subscriber's connection [for example, DSL service] is improved [see BACKGROUND of

Senapati].

       As per Claim 25, Yoshimoto teaches,

       A communication device for a communication system for performing data transmission via a

subscriber's connection in an Ethernet communication network [see network cable **101** in FIG.1; and for

example, col.3, lines 42-47] comprising: a connection data including a port identification that uniquely

identifies a subscriber's connecting line corresponding to the subscriber's connection [see abstract,

ACQUIRE TERMINAL IDENTIFIER FROM SERVICE REQUEST S201 in FIG.2, **ACQUIRE TERMINAL**

IDENTIFIER FROM CONNECTION REQUEST S301 in FIG.3 and **IDENTIFIER ACQUSITION MODULE**

in FIGS.6 and 7];

       a transmitter that is allocated to the communication device and transmits the connection data and

the subscriber data to the communication network [see **FIG.1**- *where Yoshimoto discloses **servers 102***

and clients 103, 105 & 106]; and

       an authenticator [see **AUTHENTICATION SERVER** in FIG.1] located in the communication

network that verifies authenticity of a session via the subscriber's connecting line by using the connection

data and the subscriber data, wherein the connection data and the subscriber data is transmitted via the

subscriber's connection in accordance with a predefined protocol for the Ethernet communication network

comprising at least a discovery stage to establish a session based on data supplied in one or more

discovery messages transmitted via the subscriber's connection to the communication network [see

FIGS.1-5 – *where Yoshimoto discloses transmitting client's service requests to server over network*

connection cable 101],

       wherein the authenticator [see **AUTHENTICATION SERVER** in FIG.1] is configured to

authenticate a session [**service/connection request**] via the subscriber's connection by using the

combination of the connection data [**terminal identifier**] and the subscriber data [**user identifier**]

contained in said one or more discovery messages [see **SERVICE/CONNECTION REQUEST** in FIGS.2-

5], wherein the session is established upon a joint verification of the connection data and the subscriber data which in combination identify the subscriber's connection, said joint verification [see **DECIDE CORRESPONDING AUTHORITY OF SERVER TERMINAL** in FIGS.2-5] of the connection data and the subscriber data enhancing a likelihood of accurately authenticating the session through the subscriber's connection [see for example, col.1, lines 59 to col.2, line6],

Yoshimoto discloses a subscriber data including user identifier, wherein the connection data and the subscriber data constitutes a combination of data that uniquely identifies the subscriber's connection [see **ACQUIRE USER IDENTIFIER FROM SERVICE REQUEST S202-S401** in FIGS.2 & 4, **ACQUIRE USER IDENTIFIER FROM CONNECTION REQUEST S302-S501** in FIGS.3 & 5 and **IDENTIFIER ACQUSITION MODULE** in FIGS.6 and 7]; but fails to disclose a user name and a password, and wherein the connection data and the subscriber data are inserted as respective tags into said one or more discovery messages.

However, Senapati teaches a user name and a password [see **Generic Password 234, User Identifier 238, Usernames 240, ...** in FIG.2], and wherein the connection data and the subscriber data are inserted as respective tags into said one or more discovery messages [see **Modem 104** in FIGS.1 and 2; and for example, par.0047 and 0063-0071 of **Senapati**].

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of Applicants' invention, to modify the system of Yoshimoto by incorporating Senapati's teaching, so that security of subscriber's connection [for example, DSL service] is improved [see BACKGROUND of **Senapati**].

As per Claim 14, Yoshimoto-Senapati combination teaches,
wherein the connection data is stored in the communication network [see FIGS. 6 and 7; and for example, col.8, line 53 to col.9, line 34 of **Yoshomito**].

As per Claim 16, Yoshimoto-Senapati combination teaches,

wherein the subscriber's connection is allocated to a switching device located in the communication network [see FIGS.4 and 5; and for example, col.7, line 10 to col.8, line 21 - *where* **Yoshimoto** *discloses a relay server*],

wherein the connection data and the subscriber data are inserted into said one or more discovery messages through the switching device [see **Modem 104** in FIGS.1 and 2; and for example, par.0047 and 0063-0071 of **Senapati**],

wherein said one or more discovery messages [see **SERVICE/CONNECTION REQUEST** in FIGS.2-5] which contains the connection data and the subscriber data are transmitted to an access network element located in the communication network [see FIGS.1-5 – *where Yoshimoto discloses transmitting client's service requests to server over network connection cable 101*],

wherein the respective tags which represents the connection data and the subscriber data contained in the messages is extracted in the access network element [see FIGS.1 and 2 of **Senapati** and FIGS.2-5 of **Yoshimoto**], and

wherein the extracted connection data and the subscriber data [see **IDENTIFIER ACQUISITION MODULE** in FIGS.6 and 7 of **Yoshimoto**] are transmitted from the access network element to an authentication network element located in the communication network [see FIG.1 of **Yoshimoto**] where the joint verification of the connection data and the subscriber data is performed [see FIGS.2-5 of **Yoshimoto**].

As per Claims 24 and 26, Yoshimoto-Senapati combination teaches,

wherein the subscriber's connection and the transmitter are allocated to a switching device located in the communication network [see FIGS.1, 4 & 5; and for example, col.7, line 10 to col.8, line 21 - *where* **Yoshimoto** *discloses relay server*]; and wherein the subscriber's connecting line is a wire connecting line through which the subscriber is physically connected to the communication network [see network cable **101** in FIG.1 of **Yoshimoto**].

Conclusion

8.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2139)

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139